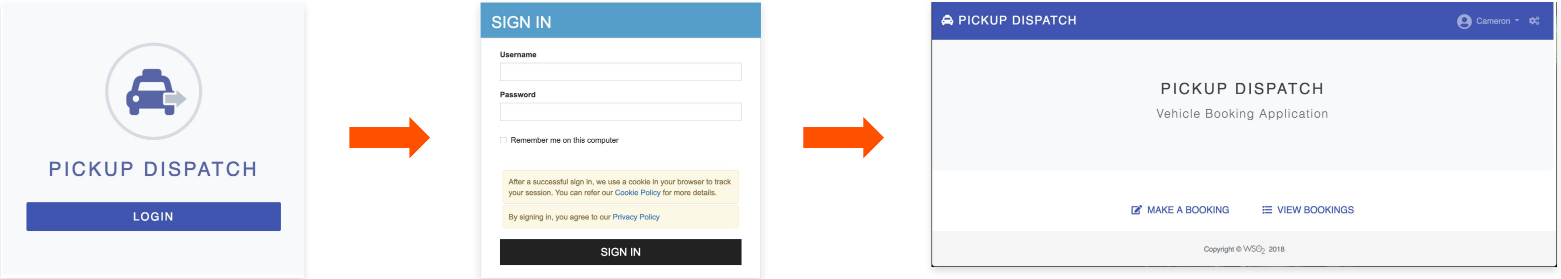
Strong Authentication with Passwordless Authentication

Authentication

What is Authentication?

- Authentication is the process used to distinctly identify a certain entity using:
  - **Knowledge factor**: Something the user knows, e.g., password, PIN, and security question.
  - **Ownership factor**: Something the user has, e.g., ATM card, identity card, mobile phone, and security token.
  - **Inherence factor**: Something the user is/does, i.e., biometrics.



After a successful sign in, we use a cookie in your browser to track your session. You can refer our Cookie Policy for more details.

By signing in, you agree to our Privacy Policy

Copyright © WSO2 2018

Benefits of Passwordless Authentication

- Increased Security and user experience
- Lower support costs
- Enhanced privacy
- Reduced Friction in the authentication process
- Future-Proof and accessible
- Helps with compliance
- Versatility and Adaptability

Passwordless authentication mechanisms

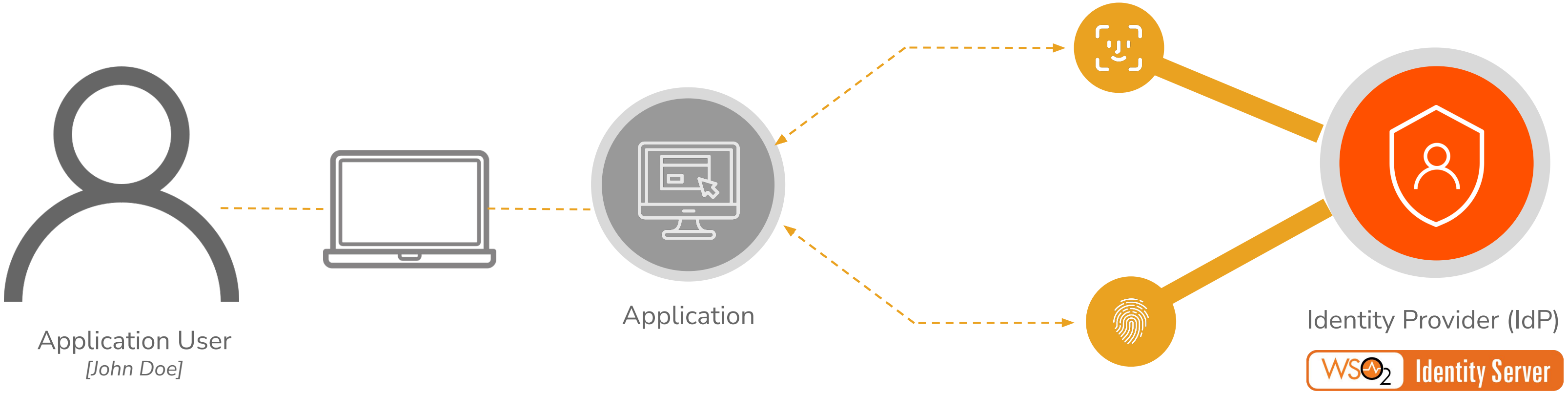
- Passkeys
- Magic Link Authentication
- Email OTP Authentication
- SMS OTP Authentication

Passkeys

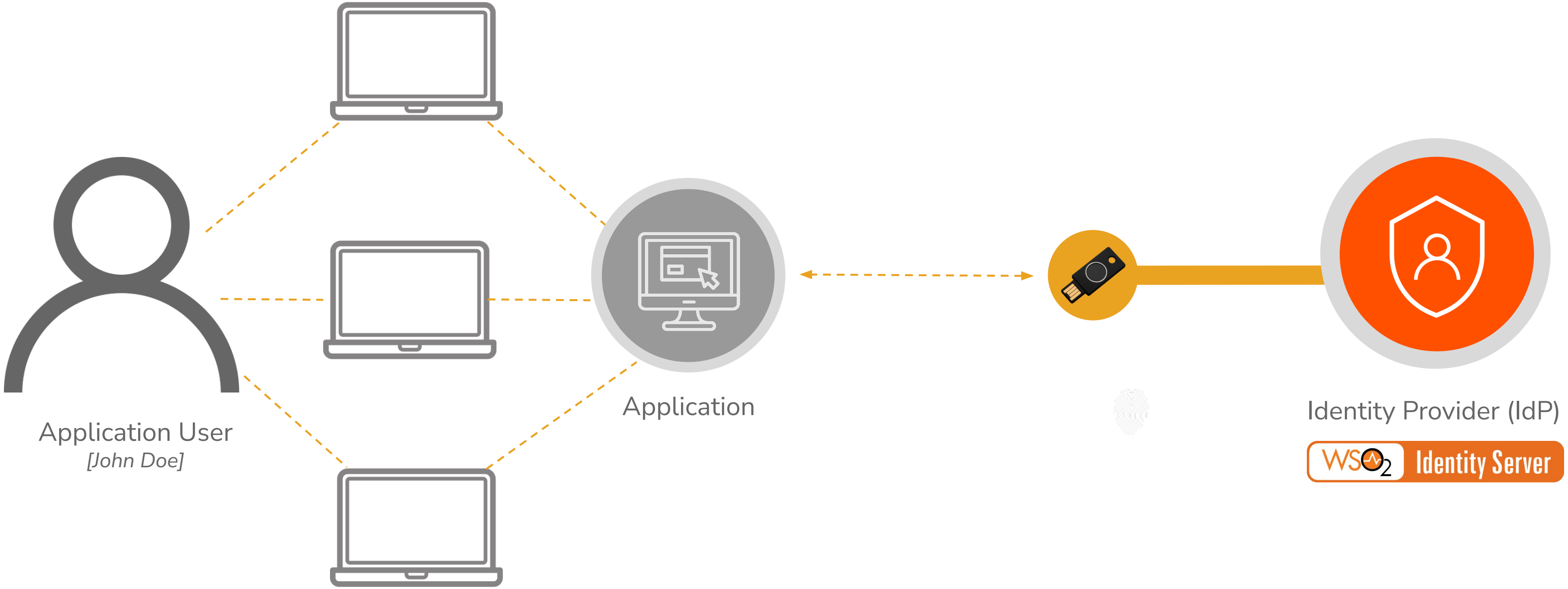
Passkeys

- Based on FIDO concepts.
- Authenticates users using two types of authenticators
  - Platform authenticators
  - Roaming authenticators
- Uses public key cryptography under the hood.
- Stored on a device and can be shared with other devices through the cloud or by scanning a QR code

Platform Authenticators

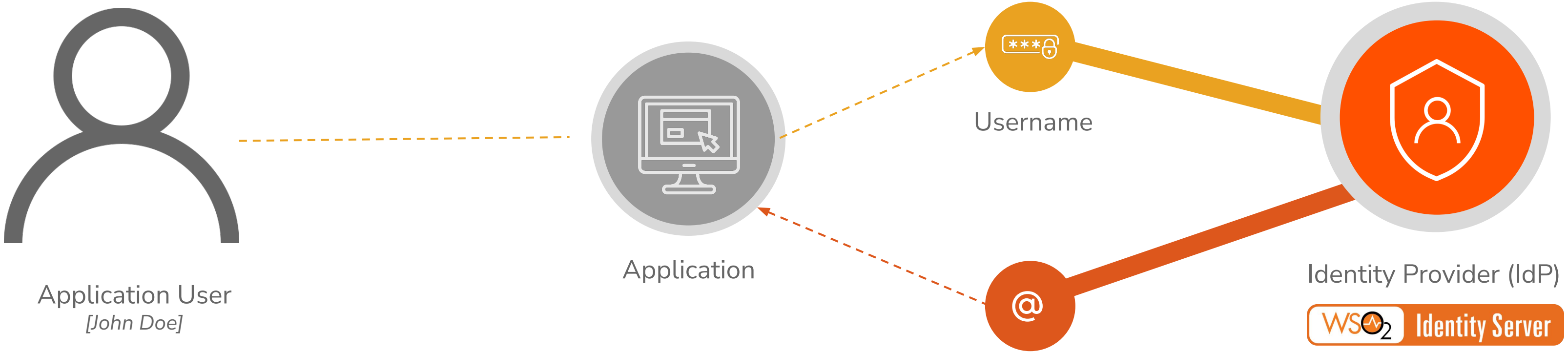


Roaming Authenticators



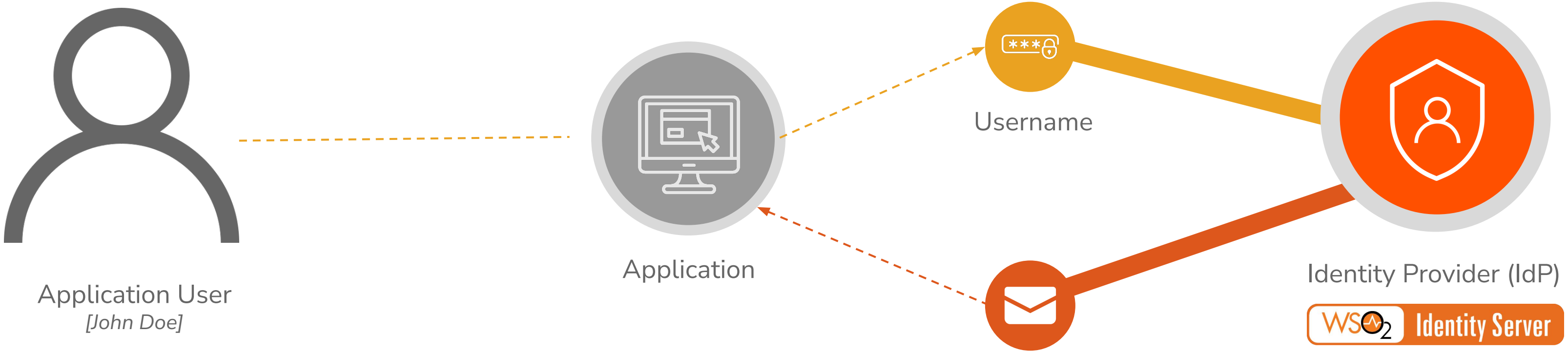
Magic Link Authentication

Magic link Authentication



SMS/ Email OTP

SMS / Email OTP Authentication



Quick Recap

What you learnt

1. About authentication
2. Benefits of using passwordless authentication
3. Passwordless authentication mechanisms

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2-identity-server

https://discord.com/invite/Xa5VubmThw

Thanks!

wso2.com